FIG.1

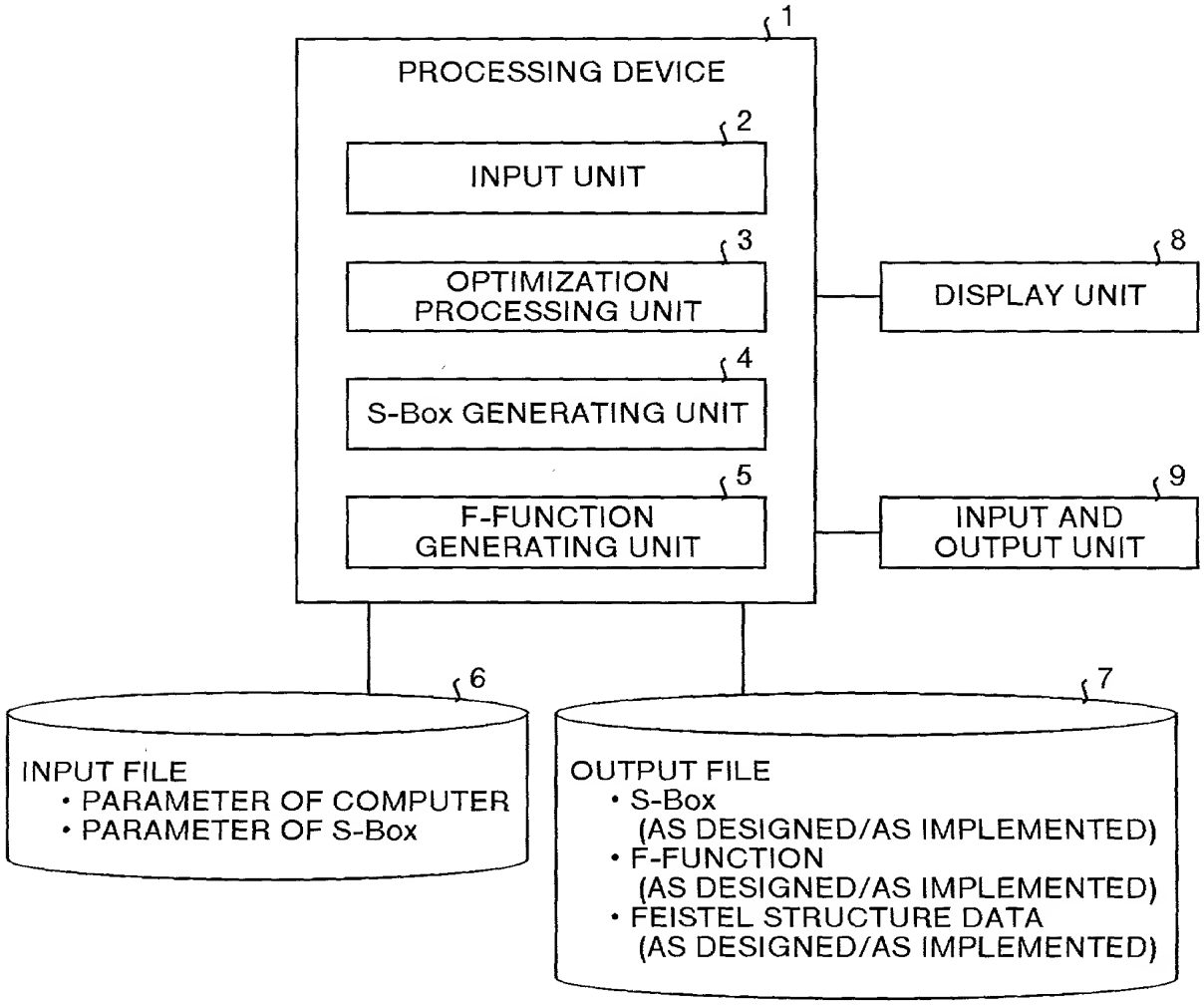
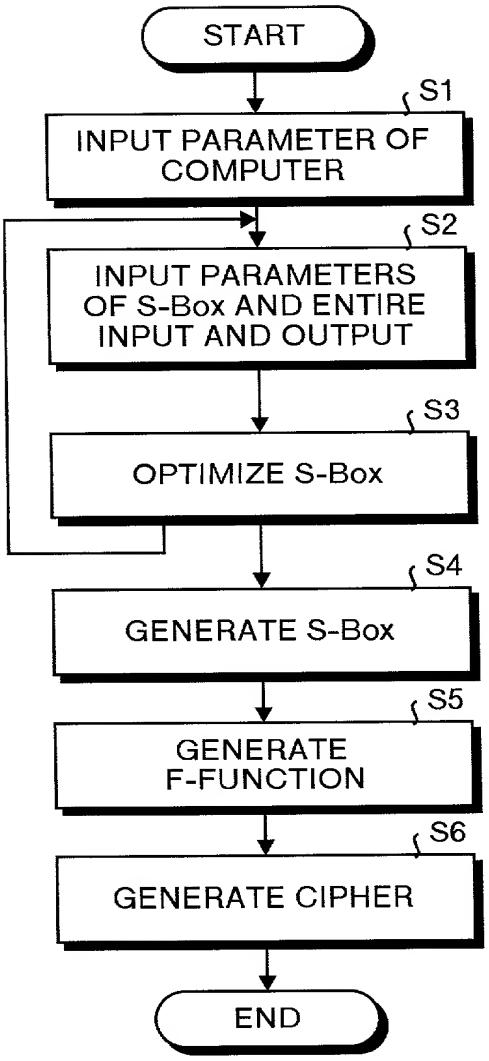


FIG.2



MEMORY CAPACITY OF PRIMARY CACHE
(1) Pentium II PROCESSOR-16 KBYTES
(2) PA-RISC PROCESSOR-1 MBYTE

- INPUT AND OUTPUT NUMBER OF S-Box IS 5 BITS OR MORE
- ENTIRE INPUT AND OUTPUT NUMBER IS 32 BITS

(1) 32 → 6, 5, 5, 5, 5, 6
11 10 11

(2) 32 → 6, 5, 5, 5, 5, 6
16 16

- GENERATE SECRET KEY RELATED TO F-FUNCTION KEY HAVING THE SAME BIT NUMBER AS F-FUNCTION INPUT AND OUTPUT BIT NUMBER

FIG.3

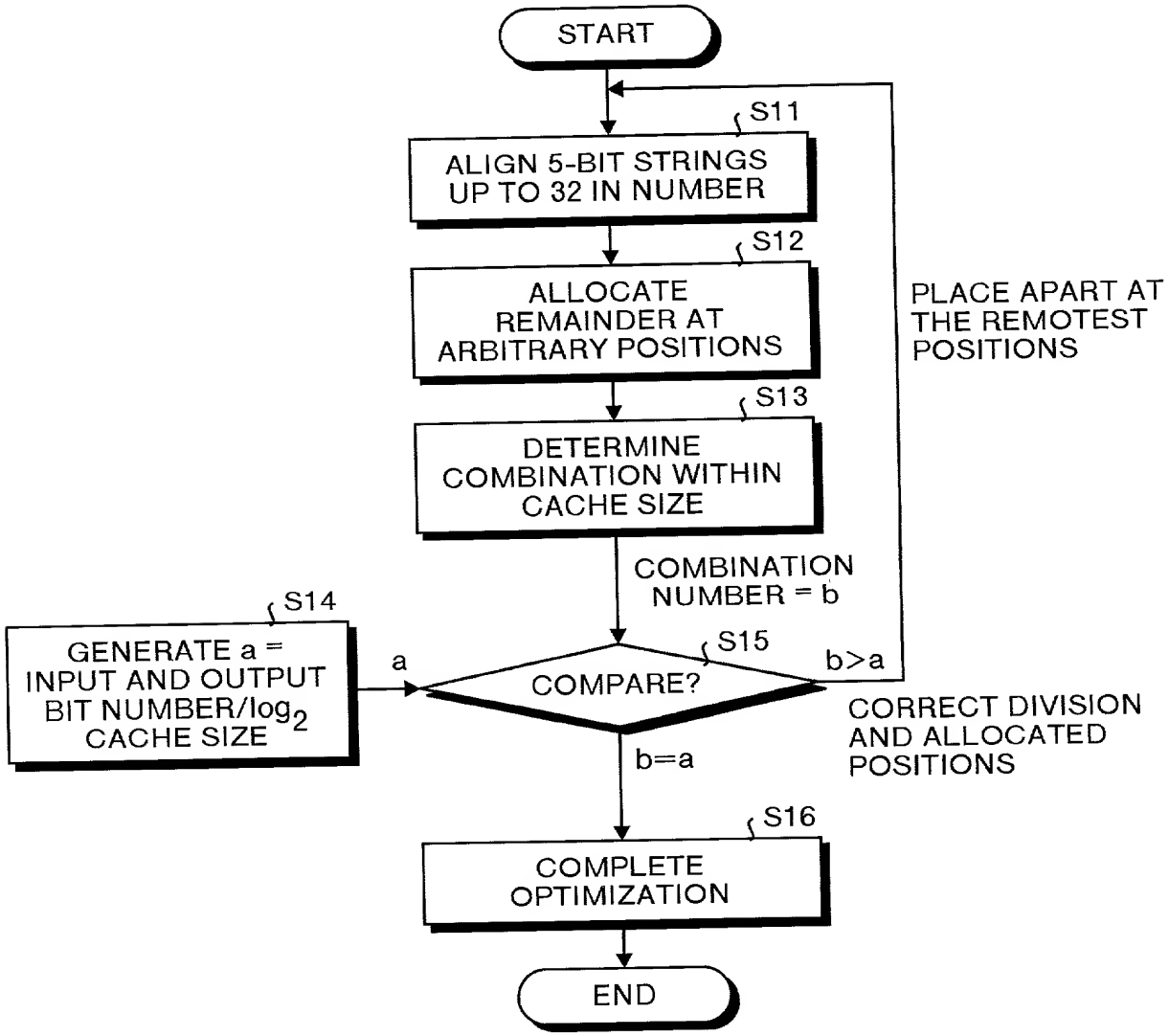

START
S11
ALIGN 5-BIT STRINGS UP TO 32 IN NUMBER
S12
ALLOCATE REMAINDER AT ARBITRARY POSITIONS
S13
DETERMINE COMBINATION WITHIN CACHE SIZE
COMBINATION NUMBER = b
S14
GENERATE a = INPUT AND OUTPUT BIT NUMBER/log2 CACHE SIZE
a
S15
COMPARE?
b>a
PLACE APART AT THE REMOTEST POSITIONS
CORRECT DIVISION AND ALLOCATED POSITIONS
b=a
S16
COMPLETE OPTIMIZATION
END

FIG.4

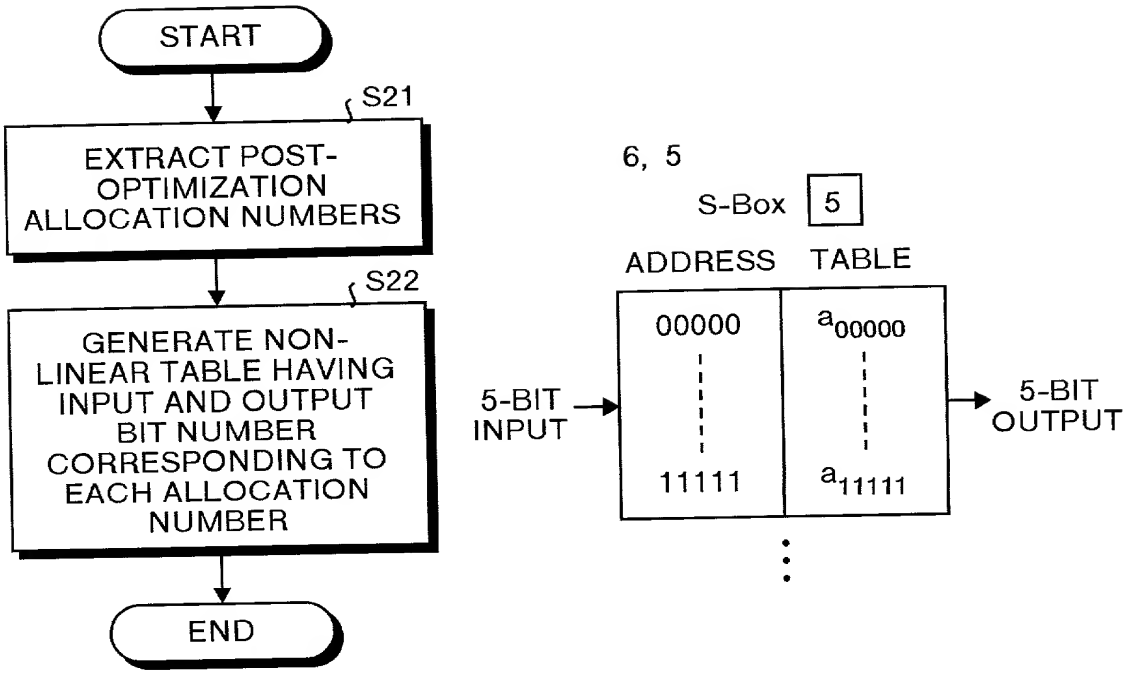

START
S21
EXTRACT POST-OPTIMIZATION ALLOCATION NUMBERS
S22
GENERATE NON-LINEAR TABLE HAVING INPUT AND OUTPUT BIT NUMBER CORRESPONDING TO EACH ALLOCATION NUMBER
END
6, 5
S-Box 5
ADDRESS
TABLE
00000
11111
a_{00000}
a_{11111}
5-BIT INPUT
5-BIT OUTPUT

FIG.5

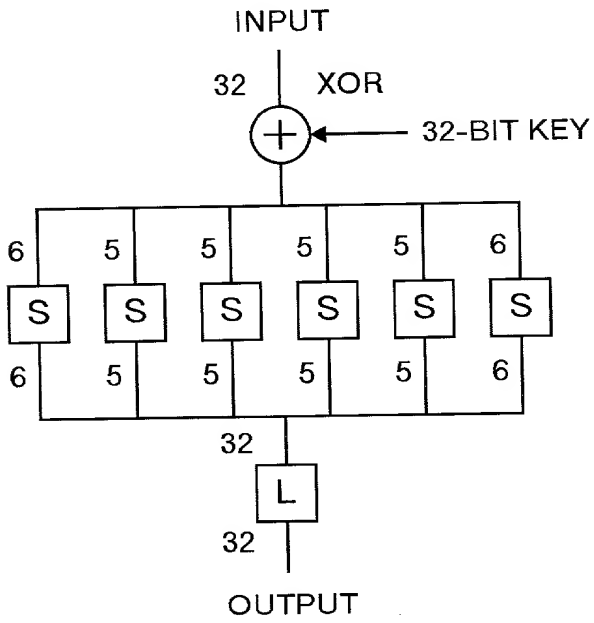

INPUT
32
XOR
32-BIT KEY
6
5
5
5
5
6
S
S
S
S
S
S
6
5
5
5
5
6
32
L
32
OUTPUT

FIG.6

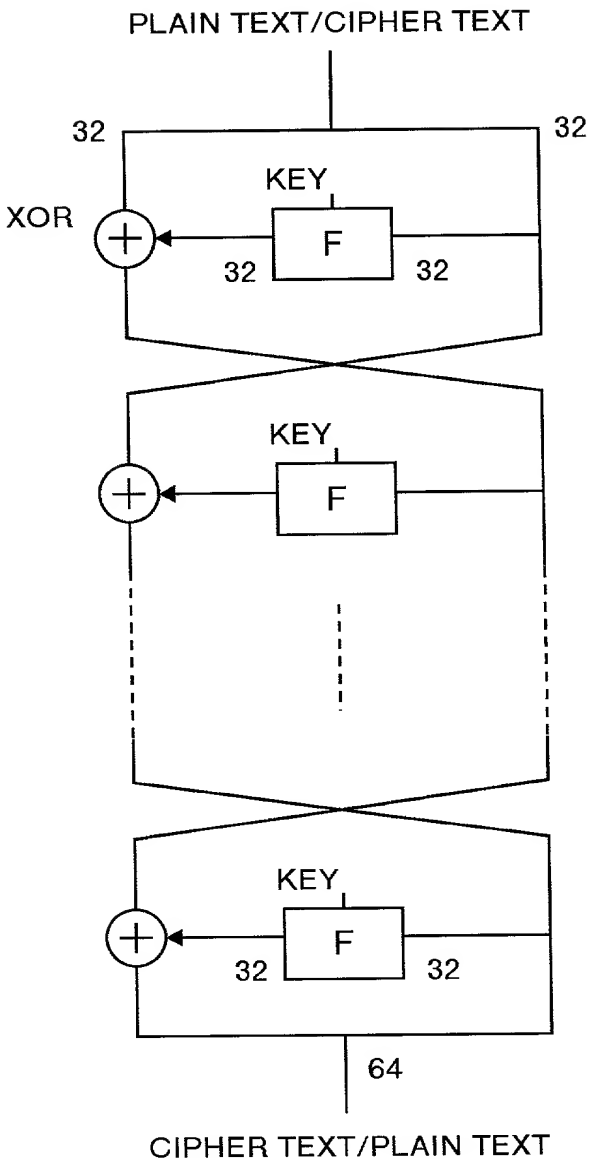

PLAIN TEXT/CIPHER TEXT
32
32
KEY
XOR
F
32
32
KEY
F
KEY
F
32
32
64
CIPHER TEXT/PLAIN TEXT

FIG.7

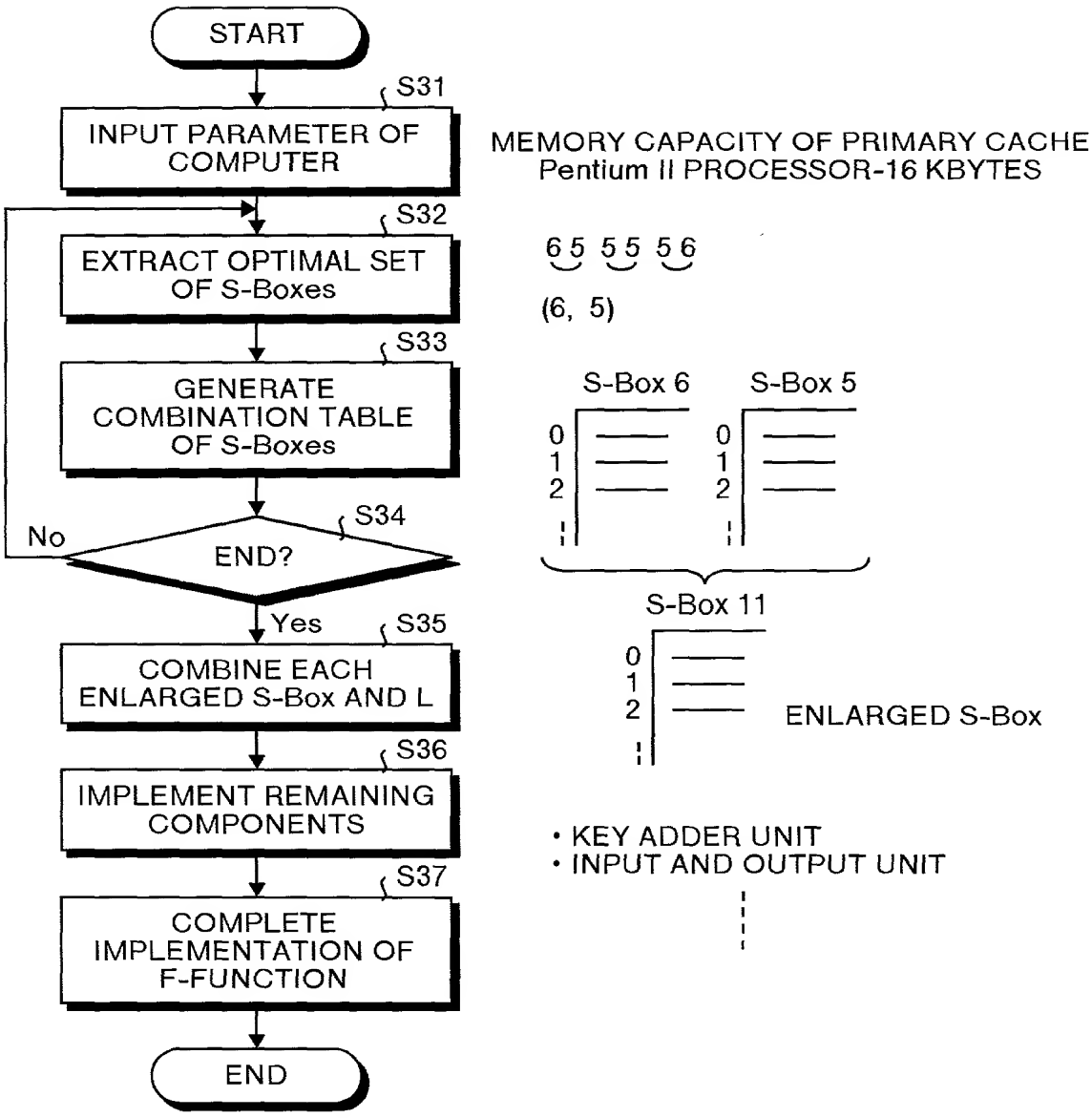

START
S31
INPUT PARAMETER OF COMPUTER
S32
EXTRACT OPTIMAL SET OF S-Boxes
S33
GENERATE COMBINATION TABLE OF S-Boxes
S34
No
END?
Yes
S35
COMBINE EACH ENLARGED S-Box AND L
S36
IMPLEMENT REMAINING COMPONENTS
S37
COMPLETE IMPLEMENTATION OF F-FUNCTION
END
MEMORY CAPACITY OF PRIMARY CACHE
Pentium II PROCESSOR-16 KBYTES
6 5 5 5 5 6
(6, 5)
S-Box 6
S-Box 5
0
1
2
S-Box 11
ENLARGED S-Box
• KEY ADDER UNIT
• INPUT AND OUTPUT UNIT

FIG.8

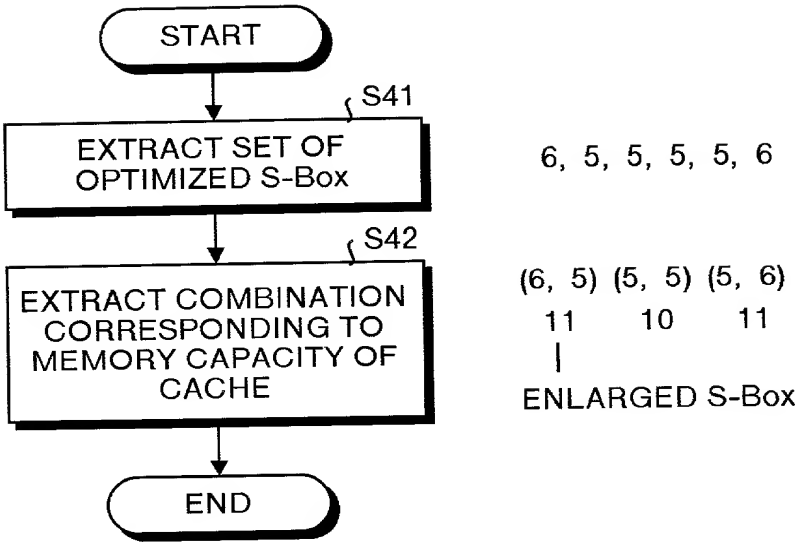

START
S41
EXTRACT SET OF OPTIMIZED S-Box
6, 5, 5, 5, 5, 6
S42
EXTRACT COMBINATION CORRESPONDING TO MEMORY CAPACITY OF CACHE
(6, 5) (5, 5) (5, 6)
11 10 11
ENLARGED S-Box
END

FIG.9

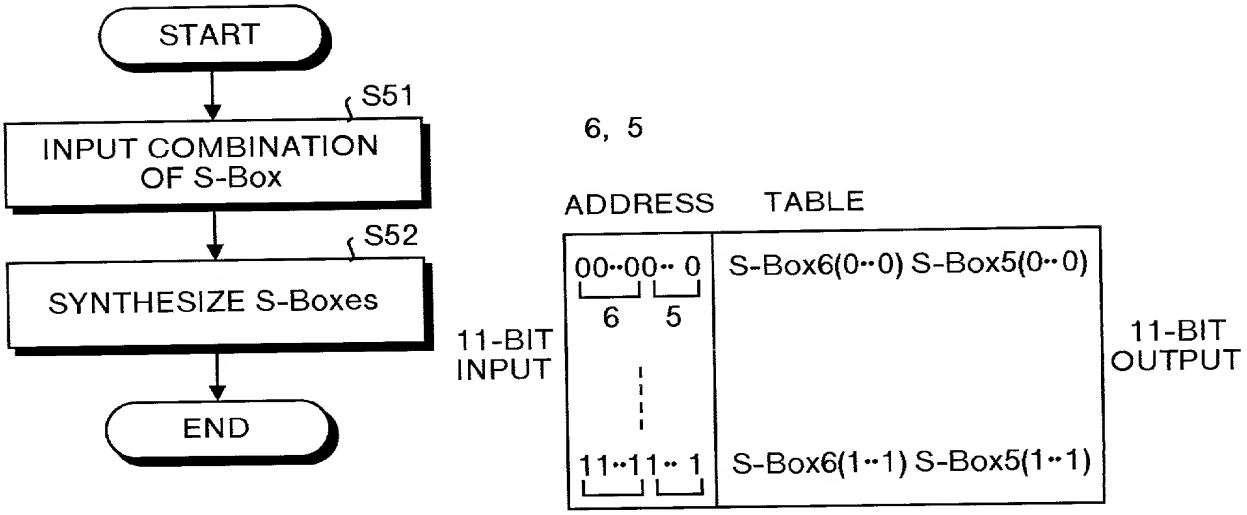

START
S51
INPUT COMBINATION OF S-Box
6, 5
ADDRESS TABLE
S52
SYNTHESIZE S-Boxes
00··00·· 0
6 5
S-Box6(0··0) S-Box5(0··0)
11-BIT INPUT
11-BIT OUTPUT
11··11·· 1
S-Box6(1··1) S-Box5(1··1)
END

FIG.10

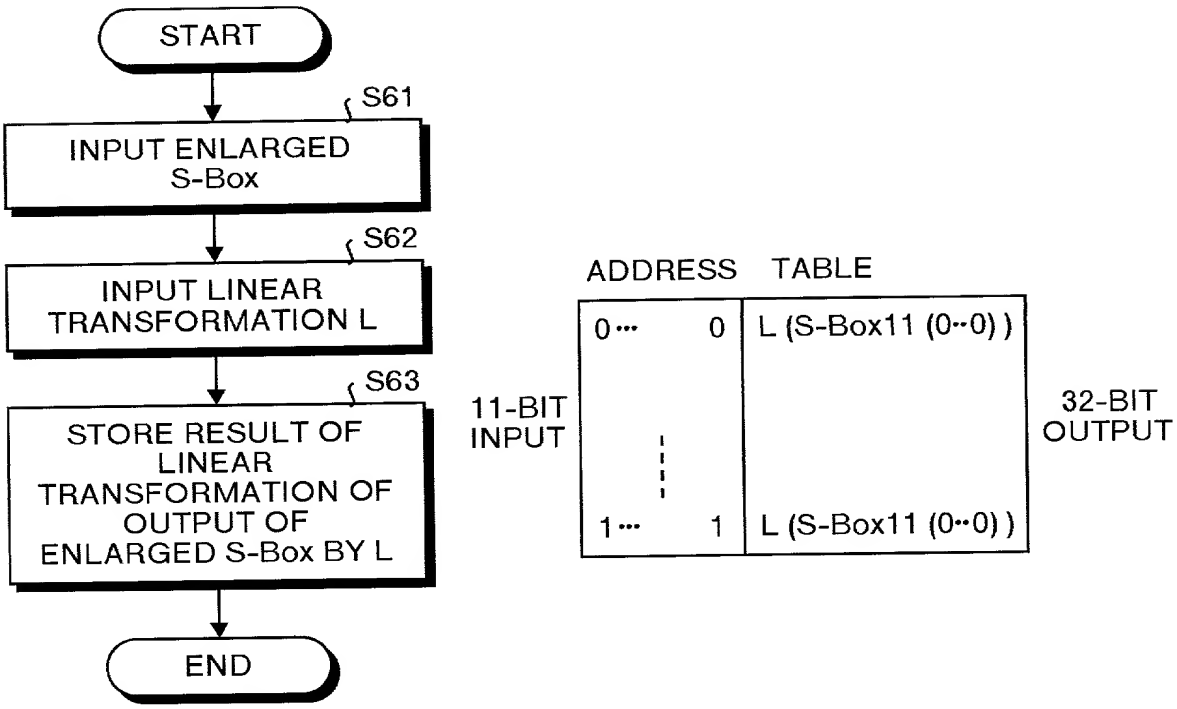
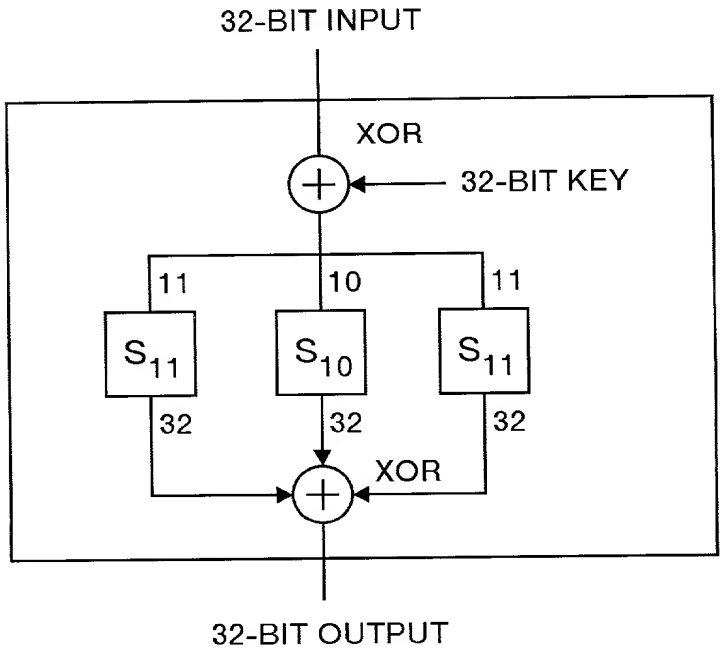

START
S61
INPUT ENLARGED S-Box
S62
INPUT LINEAR TRANSFORMATION L
S63
STORE RESULT OF LINEAR TRANSFORMATION OF OUTPUT OF ENLARGED S-Box BY L
END
ADDRESS
TABLE
11-BIT INPUT
0 ··· 0
L (S-Box11 (0··0))
1 ··· 1
L (S-Box11 (0··0))
32-BIT OUTPUT

FIG.11


32-BIT INPUT
XOR
32-BIT KEY
11
10
11
S11
S10
S11
32
32
32
XOR
32-BIT OUTPUT